UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/566,393 | 01/27/2006 | Junbiao Zhang | PU030228 | 3745 |

24498 7590 11/24/2009

Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

| EXAMINER | |
|---|---|
| SIMS, JING F | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2437 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/24/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/566,393 | ZHANG, JUNBIAO | |
| | Examiner | Art Unit | |
| | JING SIMS | 2437 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *03 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) *14-24,35 and 37-40* is/are withdrawn from consideration.

5)☐ Claim(s) *3-5,7-9,11-13,27-34,36 and 41* is/are allowed.

6)☐ Claim(s) *1,2,6,10,25,26 and 42-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This written action is responding to the Appeal Brief dated 8/3/2009.

2. In view of the Appeal Brief filed on 8/3/2009, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**4. Claims 48-57 are rejected under 35 U.S.C. 102(b) as being anticipated by Levergood et al. (US 5708780, hereinafter Levergood).**

**As per claim 48**, Levergood discloses a method for controlling network access, said method comprising *(col. 3, line 8-9, methods of processing service requests from a client to a server through a network)*:

receiving a re-directed request for network access via a message *(col. 3, line 27-29, content server initiates the authorization routine by redirecting the client's request to an authentication server)*;

transmitting a client identifier and unique data *(col. 5, line 49-65, an SID provided from the authentication server to the client. The SID includes 22-bit user identifier, and other specific data; wherein 22-bit user identifier correspond with client identifier; other data, such as 32-bit signature etc. correspond with unique data)*; and

generating a web page including embedded data *(col. 3, line 62-65, the browser generates the new web page by rewriting the current URL to replace the old name, the new URL retains SID; wherein SID that embedded in URL of the webpage correspond with a web page including embedded data)*.

**As per claim 49**, claim 48 is incorporated and Levergood discloses:

wherein said unique data comprises a session identifier and a random number *(col. 5, line 54-65, wherein 16-bit expiration date, and/or 2-bit key identifier, and or 8-bit domain correspond with session identifier; the digital signature which is a cryptographic hash of the remaining items in the SID correspond with a random number)*.

**As per claim 50**, claim 48 is incorporated and Levergood discloses:

wherein said embedded data comprises a session identifier, a random number and authentication server selection information (col. 5, line 48-65, wherein a modified URL appended with an SID correspond with embedded data; 1-bit expiration data, *and/or 2-bit key identifier, and or 8-bit domain correspond with session identifier; the digital signature which is a cryptographic hash of the remaining items in the SID correspond with a random number ; the authorized IP address correspond with authentication server selection information)*.

**As per claim 54**, Levergood discloses a method for controlling network access, said method comprising *(col. 3, line 8-9, methods of processing service requests from a client to a server through a network)*:

receiving an authentication user input message *(col. 6, line 36-41, authentication server receives a request from client)*;

transmitting authentication input page requesting authentication information *(col. 6, line 44-49, sends a challenge response which causes the client browser to prompt the user for credentials)*;

receiving authentication credentials; and transmitting an authentication message indicating one of success and failure of an authentication process *(col. 6, line 58-66, and col. 7, line 1-20, upon receive the request, if the user is not cleared for authorization, a page denying access is transmitted to the client browser. If the user is qualified, the access of the resource is granted)*.

**As per claim 55**, claim 54 is incorporated and Levergood discloses:

wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number *(col. 6, line 5-16, the authentication request get URL contains a SID, and User IP. From line col. 54 to 64, Levergood teaches that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. User IP is considered as session identifier. Since the SID is encoded the data it includes a random number)*.

**Claims 51-53** are system claims corresponding to the method claims 48-50 and therefore are rejected under the same reasons set forth in the rejections for claims 48-50.

**Claims 56-57** are system claims corresponding to the method claims 54-55 and therefore are rejected under the same reasons set forth in the rejections for claims 54-55.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**6. Claims 1, 2, 6, 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Neill (US 2004/0047348) in view of Jones et al (US 2003/0212800, hereinafter Jones).**

**As per claim 1**, O'Neill discloses a method for controlling access to a network, said method comprising:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client *(fig. 11,and [0048], wherein mobile node MN 910 correspond with the client, first Access Node FA 920 correspond with access point, AP)*;

re-directing, by said AP, said access request to a local server *(fig. 11, and [0049], wherein First Home Agent HA 930 correspond with Local server; process 970b correspond with re-directing)*;

associating unique data with an identifier of said client and storing a mapping of said association in said AP *(fig. 11, and [0047], wherein binding table 933 correspond with associating, the MIP related to End Node 910 correspond with identifier of said client, and Host Home Address HoA correspond with Unique data)*;

transmitting an authentication request to said selected authentication server *(fig. 11,and [0048], send a message 906a to AAA, Authentication, Authorization and Accounting, server 905; wherein RADIUS access_request to the AAA system 905 correspond with authentication request)*; and

receiving a response to said authentication request from said selected authentication server *(fig. 11,and [0048], a multitude of Policy state to be returned to F A 920 proves the authentication request has been received at RADIUS server)*.

However, O'Neill does not disclose:

generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client;

Jones discloses:

generating a Web page by said local server requesting that said client select an authentication server (AS) *(page 5, [0059], wherein web server correspond with local server, authentication-invite web page correspond with web page; [0060], web page can include a field for a user to select a service provider from among those available)* and including said unique data and forwarding said generated Web page to said client *([0060], wherein SIP address, password, and/or other credentials correspond with unique data)*.

O'Neill and Jones are analogous art because they are from the same field of endeavor of wireless communication access control.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the verification process of a mobile node as described by O'Neill and add giving user options to select a service provider as taught by Jones because it would provide mobile device user an other choice to connection to Internet while in the range of an hot spot.

**As per claim 2**, claim 1 is incorporated and O'Neill discloses:

wherein said network is a wireless Local Area network (WLAN) *(fig. 11 and [0002], mobile communications)*.

**As per claim 6**, claim 1 is incorporated and O'Neill discloses:

wherein said identifier is an address of said client *(fig. 11, and [0047], MIP is mobile IP which is an address of an end note/user)*.

**As per claim 10**, claim 1 is incorporated and O'Neill discloses:

wherein said identifier is one of a physical (PHY) address of said client, a MAC address of said client and an IP address of said client *(fig. 11, and [0047], MIP is mobile IP of an end note/user)*.

**7. Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Neill in view of Henry et al (US Patent No.: US 6856800 B1, hereinafter Henry).**

**As per claim 25**, O'Neill discloses a system for controlling access to a network comprising:

a client *(fig. 11, and [0048], wherein mobile node MN 910 correspond with the client)*;

an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client *(fig. 11,and [0048], wherein mobile node MN 910 correspond with the client, first Access Node FA 920 correspond with access point, AP; fig. 11, and [0049], wherein First Home Agent HA 930 correspond with Local server)*; and

an authentication server for performing an authentication process in response to a request from the client *(fig. 11,and [0048], send a message 906a to AAA, Authentication, Authorization and Accounting, server 905; wherein RADIUS access_request to the AAA system 905 correspond with authentication request)*; wherein

the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association *(fig. 11, and [0047], wherein binding table 933 correspond with associating, the information in MIP related to End Node 910 correspond with identifier of said client, and Host Home Address HoA correspond with Unique data)*;

the LS transmits the unique data to the client *(fig. 11, and [0050], lines 25-30, packet flow 960a from HA 930 to FA 920 includes packets destined for either the HoA 1 or HoA2 of the MN 910, wherein HoA 1 or HoA2 correspond with unique data)*;

the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client *(fig. 11, [0047], lines 6-16, Authorization and Authentication system 905 enables the FA to authenticate the Mobile node 910; and [0048], wherein HoA correspond with unique data)*, the AP receiving authentication parameters from the client and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation *(fig. 11, and page 7, [0047], lines 7-12, wherein binding table correspond with the mapped association data )*.

However, O'Neill does not disclose the authentication server provides a redirect header including a digitally signed authentication, and AP receiving the digitally signed retrieved re-directed URL.

Henry discloses:

the authentication server provide a redirect header including a digitally signed authentication, and AP receiving the digitally signed retrieved re-directed URL *(fig. 3, and Abstract; the security certificate is signed with a private key for the remote authentication server; the access point locally validates the authentication credential by accessing the public key of the remote authentication server from a local database, and checking the signature and expiration time of the security certificate)*.

O'Neill and Henry are analogous art because they are from the same field of endeavor of wireless communication access control.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the verification process of a mobile node as described by O'Neill and add access point receiving an digitally signed authentication certificate from authentication server as taught by Henry because it would provide access point locally validates the authentication credential and checking the signature and expiration time of the security certificate *(fig. 3, and Abstract)*.

**As per claim 26**, claim 25 is incorporated and O'Neill discloses:

wherein the network is a wireless local area network (WLAN) comprising the access point and local server *(fig. 11 and [0002], mobile communications; and [0048]-[0049], wherein first Access Node FA 920 correspond with access point, AP and First Home Agent HA 930 correspond with Local server)*.

**8. Claim 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones in view of Claxton et al (US Patent No. 7177839, hereinafter Claxton).**

**As per claim 42**, Jones discloses a method for controlling network access, said method comprising:

receiving a request for network access *(fig. 3 and [0010], mobile station request to access the network)*;

re-directing said request via a message *(fig. 3 and [0010], wherein forwarding to the designated service provider correspond with re-directing request)*;

receiving a client identifier and unique data *(fig. 3 and [0060], wherein SIP address correspond with client identifier, password and/or other credentials correspond with unique data)*;

associating said unique data and said client identifier *(fig. 3 and [0062], wherein translation table correspond with associating)*;

receiving a re-directed universal resource locator included embedded information *(page 5, [0059], authentication-invite web page correspond with re-directed universal resource locator; [0060], wherein SIP address, password, and/or other credentials correspond with embedded data)*;

However, Jones does not explicitly disclose:

generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

comparing said local digital signature with a digital signature received in said embedded information;

granting network access if said local digital signature matches said digital signature received in said embedded information; and

deny network access if said local digital signature does not match said digital signature received in said embedded information.

Claxton discloses:

generating a local digital signature using said embedded information and said association between said unique data and said client identifier *(col. 51, lines 28-30, using public keys in their partner's certificate to regenerate a signature)*;

comparing said local digital signature with a digital signature received in said embedded information *(col. 51, lines 28-30, regenerate and compare signatures*;

granting network access if said local digital signature matches said digital signature received in said embedded information *(col. 51, lines 31-38, 56-65, if the account and SSL client certificates are valid, finally give access)*; and

deny network access if said local digital signature does not match said digital signature received in said embedded information *(col. 51, lines 31-38, 56-65, if the RM client is not authenticated, the request access denies)*.

Jones and Claxton are analogous art because they are from the same field of endeavor of electronic transaction system including an access point.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the allowing multiple service providers to serve users via a wireless local access network as described by Jones and add integrity verification to messages as taught by Claxton because it would achieve transport-level integrity and data privacy *(see Claxton, col. 51, lines 10-15)*.

**9. Claims 43 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones in view of Claxton, and further in view of Chinnaswamy et al (US Publication No.: 2005/0114680).**

**As per claim 43**, claim 42 is incorporated and Chinnaswamy discloses:

wherein said unique data comprises a session identifier and a random number *([0043], the message contains random number and session identifier)*.

Jones, Claxton, and Chinnaswamy are analogous art because they are from the same field of endeavor of electronic transaction system including an access point.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the allowing multiple service providers to serve users via a wireless local access network with integrity verification system as described by Jones in views of Claxton, and add data submitting for authentication including random number and Session ID as taught by Chinnaswamy because it would provide submitting details of the access control process.

**As per claim 44**, claim 42 is incorporated and Chinnaswamy discloses:

wherein said embedded information further comprises a session identifier and authentication parameters *([0043], the message contains random number and session identifier; wherein MAC_RAND and/or random number correspond with authentication parameters)*.

Jones, Claxton, and Chinnaswamy are analogous art because they are from the same field of endeavor of electronic transaction system including an access point.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the allowing multiple service providers to serve users via a wireless local access network with integrity verification system as described by Jones in views of Claxton, and add data submitting for authentication including random number and Session ID as taught by Chinnaswamy because it would provide submitting details of the access control process.

10. **Claims 45-47** are system claims corresponding to the methods claims 42-44 and therefore are rejected under the same reasons set forth in the rejections for claims 42-44.

### *Allowable Subject Matter*

11. **Claims 3-5, 7-9, 11-13, 34, 36, and 41** are allowed.

12. **Claims 27-33** are allowed.

### *Examiner Notes*

13. Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

***Conclusion***

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JING SIMS/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437